

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Pennsylvania

In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*

LG TP260 cellphone with serial number 711CYYQ687858

Case No. 18-1350-M

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Search Warrant Attachment "A" incorporated herein.

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

See Search Warrant B incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

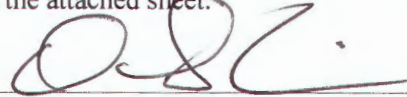
*Code Section*18 U.S.C. Sections 2251(a)  
and 2252(a)(4)*Offense Description*

Production and Possession of Child Pornography

The application is based on these facts:

See attached Affidavit incorporated herein.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of        days (give exact ending date if more than 30 days:                     ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

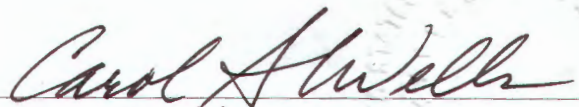
*Applicant's signature*

Daron Schreier, Special Agent, FBI

*Printed name and title*

Sworn to before me and signed in my presence.

Date:

August 23, 2018City and state: Philadelphia, Pennsylvania*Judge's signature*

Hon. Carol Sandra Moore Wells

*Printed name and title*

## **AFFIDAVIT**

I, Daron Schreier, being duly sworn, do hereby depose and state:

### **I. BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigation, and have been since January of 2006. Since August of 2006, I have been assigned to the Philadelphia Division where I have been a member of the Joint Terrorism Task Force's Cyber Squad, and most recently the Violent Crimes against Children Squad. I have received training from the FBI in the fields of international terrorism, counter-intelligence, computer crime, and the enforcement of federal child pornography laws. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

2. I make this affidavit in support of an application for a search warrant to search an LG TP260 cellphone with serial number 711CYYQ687858 seized by the Philadelphia Police Department and currently in the custody of the Federal Bureau of Investigation (hereafter "TARGET DEVICE"), which has been more fully described in Attachment "A" of this affidavit. There is probable cause to search the devices described in Attachment "A" for evidence of violations of Title 18, United States Code, Sections 2251(a) [Production of Child Pornography] and 2252(a)(4) [Possession of Child Pornography], further described in Attachment "B." The statements contained in this affidavit are based upon my investigation, information provided by other FBI agents and Law Enforcement officers, other personnel specially trained in the seizure and analysis of computers and electronic media, and on my experience and training as a Special Agent of the FBI.

3. Because this affidavit is being submitted for the limited purpose of securing a search warrant and it involves a minor, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251 and 2252 exist on the TARGET DEVICE.

### **II. APPLICABLE STATUTES AND TECHNICAL TERMS**

4. Title 18, United States Code, Section 2251(a), makes it a crime to knowingly use, employ, persuade, induce, entice, or coerce a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, and the depiction is produced using materials that had been mailed, shipped, or transported in interstate or foreign commerce.

5. Title 18, United States Code, Section 2252(a)(4)(B) makes it a crime to knowingly possess one or more matters which contain any visual depiction of a minor



engaged in sexually explicit conduct, produced using a minor engaged in such conduct, that has been mailed or that has been transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or were produced using materials that were mailed or so transported, by any means including by computer.

6. Title 18 United States Code, Section 2256(2)(A) defines “sexually explicit conduct” as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or the lascivious exhibition of the genitals or pubic area of any person.

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. *Digital camera*: A digital camera is a camera that records video and pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. *Portable media player*: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types



of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. *GPS*: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.
- e. *PDA*: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. *Tablet*: A tablet is a mobile computer, typically larger than a cell phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.



- g. *IP Address*: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static — that is, long-term — IP addresses, while other computers have dynamic — that is, frequently changed — IP addresses.
- h. *Internet*: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

8. Based on my training, experience, and research, I know that the TARGET DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA, and tablet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

### **III. COMPUTERS AND CHILD PORNOGRAPHY**

9. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

10. The development of computers has changed this. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

11. Child pornographers can now transfer photographic prints made from a film camera into a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly from a digital camera onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally hundreds of millions of computers around the world.



12. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at a very high resolution.

13. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

14. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

15. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, *i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, *e.g.*, traces of the path of an electronic communication may be automatically stored in many places on the computer (*e.g.*, temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the computer's web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer contains peer to peer software, and when the computer was sharing files. Such information may be maintained indefinitely until overwritten by other data.

16. Graphic image files containing child pornography can be maintained for long periods of time on a computer. Most often the collector maintains the files purposefully. But even when the pornographic files have been deleted (due to guilt or fear of discovery), however, computer forensic experts are nonetheless often able to recover the pornographic images that were purposefully possessed at some previous time from the computer's "unallocated" or "slack" space. In addition, pornographic images can often be recovered from the temporary Internet files, or "cache" of a computer. A forensic examiner often can recover evidence suggesting whether a computer has been used to access e-mail or chat programs, and files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

17. As stated in paragraph 8, I know that the TARGET DEVICE work much like a tablet and personal computer. Based on my training and experience, I know that



evidence of child pornography can often be found in electronic devices that function like a computer, including devices like the TARGET DEVICE.

#### **IV. CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

18. I know based on my training and experience that most individuals who are sexually attracted to children facilitate their sexual arousal through imagery that focuses, in part or in whole, on children. Specifically, these individuals often collect child pornography. These individuals may derive sexual gratification from actual physical contact with children as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude depictions of children engaged in sexually explicit conduct.

19. In addition to child pornography, these individuals are also highly likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica," which is defined as any material, relating to children, that serves a sexual purpose for a given individual. It is broader and more encompassing than child pornography, but at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his intent. It includes things such as fantasy writings, letters, diaries, drawings, cartoons and non-sexually explicit visual images of children.

20. Child pornography collectors reinforce their fantasies, often by taking progressive, overt steps aimed at turning the fantasy into reality in some or all of the following ways: collecting and organizing their child related material; masturbating while viewing the child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other likeminded adults through membership in organizations catering to their sexual preference for children thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need-driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

21. Persons with a sexual interest in children often maintain and possess their material in the privacy and security of their homes or some other secure location, such as a private office or work computer, where it is readily available. The collection may include sexually explicit or suggestive materials involving children, such as photographs,



magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images, computer videos, or other visual media. Because they put so much time and energy into obtaining the material, they do not delete or destroy their collections.

## **V. PROBABLE CAUSE**

22. On July 29, 2018, the mother of a four-year old female (hereafter "MINOR #1"), both of whose identities are known to me, observed JOSÉ LUNA-BENSCOME holding MINOR #1's hand and acting in a strange manner in the kitchen of her residence, which is located in Philadelphia, Pennsylvania. On July 30, 2018, the mother of MINOR #1 was discussing the incident with the grandmother of MINOR #1, and the grandmother reported that she also observed LUNA-BENSCOME with MINOR #1 in the kitchen and that the grandmother saw LUNA-BENSCOME fixing his pants and become nervous upon seeing the grandmother.

23. On July 30, 2018, the mother of MINOR #1 talked to MINOR #1 about LUNA-BENSCOME. MINOR #1 initially told her mother that she did not want to tell her anything. The mother of MINOR #1 told MINOR #1 she was going to check the surveillance video from within the residence, and MINOR #1 began to cry. The mother of MINOR #1 reviewed the surveillance video and observed on multiple occasions LUNA-BENSCOME opening MINOR #1's legs and touching her vaginal area. Upon seeing the video, the mother of MINOR #1 took MINOR #1 to the hospital to be checked out and reported the incident to the Philadelphia Police Department, Special Victims Unit. During an interview with Special Victims Unit detectives on July 30, 2018, the mother of MINOR #1 positively identified a photo of JOSÉ LUNA-BENSCOME as the individual seen touching MINOR #1's vaginal area in the surveillance video.

24. The mother of MINOR #1 provided the surveillance video to Special Victims Unit Detectives. I reviewed this video and found that on at least three occasions, LUNA-BENSCOME is seen pushing open MINOR #1's legs while she is wearing a bathing suit and touching her vaginal area while other children are in the room.

25. On July 30, 2018, after watching the surveillance video, the mother of MINOR #1 called LUNA-BENSCOME to confront him about the incident. LUNA-BENSCOME stayed quiet during this conversation, and did not make any admissions about his conduct. The following day, on August 1, 2018, the mother of MINOR #1 started exchanged text messages with LUNA-BENSCOME, in which she again confronted him about the incident. The mother of MINOR #1 later showed these messages to detectives, who took pictures of the text messages. The message were in Spanish, and I subsequently reviewed a translation of these messages. In summary, during the conversation LUNA-BENSCOME apologized and said he was drunk and that he felt bad and ashamed about what happened, although he denied doing anything to MINOR #1. LUNA-BENSCOME also asked the mother of MINOR #1 not to talk to anyone about the incident and thanked her for not talking to the police. The following day, on August 2, 2018, LUNA-



BENSCOME told the mother of MINOR #1 that he was going to the police to tell them everything and asked her to have the video ready to give to police.

26. On August 1 and 2, 2018, LUNA-BENSCOME attempted to contact Philadelphia Police Officer Oswaldo Toribio, who is a friend of LUNA-BENSCOME's brother. Officer Toribio called LUNA-BENSCOME on August 2, 2018, and during the conversation LUNA-BENSCOME told Officer Toribio that he "fucked up". He admitted to Officer Toribio that he had touched MINOR #1 and that he did not know what to do. LUNA-BENSCOME did not provide details about his conduct over the phone, but told Officer Toribio that he wanted to turn himself in to the police. Officer Toribio contacted Special Victims Unit and was advised to bring LUNA-BENSCOME to their office. Officer Toribio picked up LUNA-BENSCOME and drove him to the Special Victims Unit. LUNA-BENSCOME was not restrained in any manner during the car ride, and never indicated he no longer wanted to turn himself in. During the car ride, LUNA-BENSCOME told Officer Toribio that he was at MINOR #1's house for a barbeque on Sunday, July 29, 2018. LUNA-BENSCOME observed MINOR #1 in the pool and saw that her bathing suit had moved and exposed her vagina. Later, LUNA-BENSCOME went inside the house with MINOR #1 and played with her vagina. LUNA-BENSCOME told Officer Toribio that he felt very sad and wanted to pay for what he did.

27. On August 2, 2018, LUNA-BENSCOME was interviewed by Detectives Edward Enriquez and Kevin Gage at Special Victims Unit, which was audio and video recorded. LUNA-BENSCOME was advised of his *Miranda* rights, which he waived and agreed to speak with detectives. In summary, LUNA-BENSCOME made the following admissions:

- a. LUNA-BENSCOME touched MINOR #1's vagina several times on Sunday (July 29, 2018) while in MINOR #1's residence. LUNA-BENSCOME showed MINOR #1 a pornography video on his cellphone so that MINOR #1 would allow herself to be touched. LUNA-BENSCOME has shown pornography to MINOR #1 on approximately three prior occasions.
- b. LUNA-BENSCOME previously resided at MINOR #1's residence, and during this time on numerous occasions had taken MINOR #1 to the basement and touched her vagina with his hands while MINOR #1 was unclothed.
- c. On one occasion, LUNA-BENSCOME exposed his penis to MINOR #1 and had her touch his penis until he ejaculated.
- d. LUNA-BENSCOME took naked photographs of MINOR #1's private parts with his cell-phone while in the basement of MINOR #1's residence.



- e. LUNA-BENSCOME tried to erase the photographs of MINOR #1 from his cellphone, but could not do it. He confirmed the photographs would still be on the cellphone.

28. When he was brought to Special Victims Unit on August 2, 2018, LUNA-BENSCOME had in his possession the TARGET DEVICE, an LG TP260 cellphone with serial number 711CYYQ687858. This cell-phone was seized by Philadelphia Police incident to LUNA-BENSCOME's arrest. On August 3, 2018, Philadelphia Police obtained Commonwealth of Pennsylvania search warrant #212557 to search the TARGET DEVICE for certain items related to the crimes of aggravated indecent assault and sexual abuse of children. On August 3, 2018, the TARGET DEVICE was transferred to the custody of the Federal Bureau of Investigation. Pursuant to the Commonwealth of Pennsylvania search warrant, I utilized mobile forensics software to extract the contents of the TARGET DEVICE, but did not review any of the content, other than to obtain identifying information for the TARGET DEVICE.

## **VI. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

29. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order and/or with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password protected, or encrypted files. Because computer evidence is extremely vulnerable to tampering or destruction, which may be caused by malicious code or normal activities of



an operating system, the controlled environment of a laboratory is essential to its complete and accurate analysis.

## **VII. SEARCH METHODOLOGY TO BE EMPLOYED**

30. To search for electronic data contained in computer hardware, computer software, and/or memory storage devices, the examiners will make every effort to use computer forensic software to have a computer search the digital storage media. This may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. Searching for image files to locate images of children engaging in sexually explicit conduct or child erotica, examining log files associated with the receipt, transmission, and viewing of such images, examining metadata of such images, and examining all of the data contained in such computer hardware, computer software, and /or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in the search warrant;
- b. Surveying various file directories and the individual files they contain;
- c. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in the warrant (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- d. Opening files in order to determine their contents;
- e. Scanning storage areas;
- f. Searching for malware (computer code not intended by the user) in order to, if necessary, rebut a defense that malware caused the receipt, possession or distribution of child pornography;
- g. Performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment "B"; and/or
- h. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment "B."



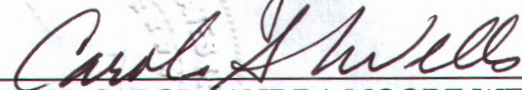
### VIII. CONCLUSION

31. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that on the TARGET DEVICE, further described in Attachment "A," there will be located evidence, contraband, and fruits and instrumentalities of violations of 18 U.S.C. §§ 2251(a) and 2252(a)(4), as further described in Attachment "B."



DARON SCHREIER  
*Special Agent*  
*Federal Bureau of Investigation*

Sworn and subscribed to before me  
this 23<sup>rd</sup> day of August 2018.



HON. CAROL SANDRA MOORE WELLS  
*United States Magistrate Judge*  
*Eastern District of Pennsylvania*



**ATTACHMENT "A"**

**DESCRIPTION OF LOCATION TO BE SEARCHED**

(Target Device)

An electronic device, originally seized by the Philadelphia Police Department, and currently maintained in the custody of the Federal Bureau of Investigation in Philadelphia, Pennsylvania, further described as

- LG TP260 cellphone with serial number 711CYYQ687858



## **ATTACHMENT "B"**

### **ITEMS TO BE SEIZED**

The following items may be searched for and seized: Evidence of violations of 18 U.S.C. §§ 2251(a), and 2252 (a)(4), including:

1. All visual depictions of minors engaged in sexually explicit conduct (as defined in 18 U.S.C. § 2256) produced using minors engaged in such conduct, on the TARGET DEVICE, including those in opened or unopened e-mails and chat conversations.

2. All documents, including correspondence, records, opened or unopened e-mails, chat logs, and internet history, pertaining to the possession, receipt, access to or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography whether transmitted or received, or which tends to show the knowing possession of any child pornography possessed, or which involves communications with minors in efforts to encourage the minors to engage in sexually explicit conduct.

3. All documents, including correspondence, records, opened or unopened e-mails, chat logs, and internet history that pertains to the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission in or affecting interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

4. All documents, including correspondence, records, opened or unopened e-mails, chat logs, and internet history which evidence operation or ownership or use of the Target Device, including, but not limited to, correspondence, sales receipts, bills for internet access, financial records, tax records, personal photographs, telephone records, notes books, diaries, reference materials, or other personal items, and registration information for any software on the computer.

5. All passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data on the Target Device. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to the operating system, individual electronic files, or other electronic data.

6. Evidence and contents of logs and files of the TARGET DEVICE, such as those generated by the computer's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person



using the TARGET DEVICE at the time any visual depictions or communications described in paragraphs 1 and 2 of this attachment were created, sent, received, or viewed. Also, any malware resident on the TARGET DEVICE.